Notice of Allowability	Application No.	Applicant(s)	
	09/851,763	RYGAARD, CHRISTOPER A.	
	Examiner	Art Unit	
	Peter Poltorak	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *papers filed on 1/13/06*.

2. ☒ The allowed claim(s) is/are *1, 3-10, 12-19, 21-28 and 30-49*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 1/13/06
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *7/05/06* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

JACQUES LOUIS-JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

1. This Office Action is in response to papers filed on 1/13/2006.
2. The papers included a request for continuation so that the submitted IDS could be considered.

Allowable Subject Matter

3. Claims 1-49 are allowed.
4. The following is a statement of reasons for the indication of allowable subject matter.
5. The closest prior art, *Ordille (Joann J. Ordille, "When agents roam, who can you trust")* discusses mobile applications jumping between hosts during execution. Although, in multiple embodiments of mobile application implementations *Ordille* teaches authentication of the user's subscription to mobile application services, mobile applications' trust level that may effect the decision of verifying the dispatching node, sensitivity of the mobile application influencing a travel path of the mobile application and a management and security console computer, *Ordille* fails to teach "determining if authentication of a user of the dispatching host is required prior to dispatch of a mobile application responsive to ... determining if the mobile application is a sensitive mobile application and determining if the dispatching node is a vulnerable node" as required by independent claims 1, 10, 19, 28, 37 and 47. In particular, *Ordille* does not teach or suggest the link between the sensitivity of a mobile application and vulnerability of a dispatching node and requiring authentication of a user of the dispatching host when it is determined that the mobile application is sensitive and that the dispatching node is vulnerable. This would not

have been obvious to one of ordinary skill in the art at the time of applicant's invention.

The prior art, fails to anticipate or fairly suggest the limitation of applicant's independent claims, in such a manner that a rejection under 35 U.S.C. 102 or 103 would be proper. As a result the claimed invention is considered to be in condition for allowance as being novel and non-obvious over prior art.

6. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Examiner Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mark Kirkland on 07/07/2006.

The application has been amended as follows:

--

1. A mobile application security system, comprising:

a management and security console computer connected to one or more hosts, each host configured to execute a mobile application that jumps between hosts during execution, the management and security console computer comprising means for

monitoring security of the mobile application as it jumps between a dispatching host and another host wherein information about the mobile application and the dispatching host is communicated to the management and security console computer, the security monitoring means further comprising means for determining if authentication of a user of the dispatching host is required prior to dispatch of the mobile application responsive to means for determining if the mobile application is a sensitive mobile application and determining if the dispatching host is a vulnerable host, and means for requesting authentication if authentication of the user is required.

2. (Cancelled)

3. The system of claim 1, wherein requesting means requests the authentication if a sensitive mobile application is being dispatched.

4. The system of claim 1, wherein requesting means requests the authentication if a mobile application is being dispatched from a vulnerable host.

5. The system of claim 1, wherein the management and security console computer further comprises means for authenticating the user based on one or more rules defined by a managing user.

6. The system of claim 1, wherein the management and security console computer further comprises means for assigning a vulnerable classification or a non-vulnerable classification to each host.

7. The system of claim 1, wherein the management and security console computer further comprises means for assigning a sensitive classification or a non-sensitive classification to each mobile application as the mobile application is created.

8. The system of claim 1, wherein each mobile application comprises an itinerary listing a node for each host to which the mobile application jumps in the mobile application system wherein each node indicates if the authentication is required to jump

from the particular host and wherein the requesting means requests the authentication based on the node in the itinerary.

9. The system of claim 1, wherein a host comprises one or more wireless devices that are classified as vulnerable.

10. A mobile application security method, comprising:

receiving data about a mobile application at a security node each time the mobile application jumps from a dispatching host to another host;

determining if authentication of a user of the dispatching host is required prior to dispatch of the mobile application, including determining if the mobile application is a sensitive mobile application and determining if the dispatching node is a vulnerable node; and

responsive to determining, requesting authentication if authentication of the user is required.

11. (Cancelled)

12. The method of claim 10, wherein requesting comprises requesting the authentication if a sensitive mobile application is being dispatched.

13. The method of claim 10, wherein requesting comprises requesting the authentication if a mobile application is being dispatched from a vulnerable host.

14. The method of claim 10, further comprising authenticating the user based on one or more rules defined by a managing user.

15. The method of claim 10, further comprising assigning a vulnerable classification or a non-vulnerable classification to each host.

16. The method of claim 10, further comprising assigning a sensitive classification or a non-sensitive classification to each mobile application as the mobile application is created.

17. The method of claim 10, wherein each mobile application comprises an itinerary listing a node for each host to which the mobile application jumps, wherein each node indicates if authentication is required to jump from the particular host and wherein requesting further comprises requesting the authentication based on the node in the itinerary.

18. The method of claim 10, wherein a host comprises one or more wireless devices that are classified as vulnerable.

19. A mobile application security system, comprising:

a management and security node connected to one or more nodes of a peer-to-peer network, each node configured to execute a mobile application, the management and security node comprising means for monitoring security of the mobile application as it jumps between the one or more nodes wherein data about the mobile application is communicated to the management and security node prior to the mobile application being dispatched from a dispatching node, the security monitoring means further comprising means for determining if authentication of a user of the dispatching node is required prior to dispatch of the mobile application responsive to means for determining if the mobile application is a sensitive application and determining if the dispatching node is a vulnerable node, and means for requesting authentication if authentication of the user is required.

20. (Cancelled)

21. The system of claim 19, wherein the requesting means requests the authentication if a sensitive mobile application is being dispatched.

22. The system of claim 19, wherein the requesting means requests the authentication if a mobile application is being dispatched from a vulnerable node.

23. The system of claim 19, wherein the management and security node further comprises means for authenticating the user based on one or more rules defined by a managing user.

24. The system of claim 19, wherein the management and security node further comprises means for assigning a vulnerable classification or a non-vulnerable classification to each node.

25. The system of claim 19, wherein the management and security node further comprises means for assigning a sensitive classification or a non-sensitive classification to each mobile application as the mobile application is created.

26. The system of claim 19, wherein each mobile application comprises an itinerary listing a node for each node to which the mobile application jumps in the mobile application system wherein each node indicates if the authentication is required to jump from the particular node and wherein the requesting means requests the authentication based on the node in the itinerary.

27. The system of claim 19, wherein a node comprises one or more wireless devices that are classified as vulnerable.

28. A mobile application security method, comprising:

receiving data about a mobile application at a management and security node each time the mobile application is being dispatched from a dispatching node in a peer-to-peer network;

determining if authentication of a user of the dispatching node is required prior to dispatch of the mobile application, including determining if the mobile application is a sensitive application and determining if the dispatching node is a vulnerable node; and

responsive to determining, requesting authentication if authentication of the user is required.

29. (Cancelled)

30. The method of claim 28, wherein requesting comprises requesting the authentication if a sensitive mobile application is being dispatched.

31. The method of claim 28, wherein requesting comprises requesting the authentication if a mobile application is being dispatched from a vulnerable node.

32. The method of claim 28, comprising authenticating the dispatching node based on one or more rules defined by a managing user.

33. The method of claim 28, further comprising assigning a vulnerable classification or a non-vulnerable classification to each node.

34. The method of claim 28, further assigning a sensitive classification or a non-sensitive classification to each mobile application as the mobile application is created.

35. The method of claim 28, wherein each mobile application comprises an itinerary listing a node for each node to which the mobile application jumps wherein each node indicates if authentication is required to jump from the particular node and wherein requesting further comprises requesting the authentication based on the node in the itinerary.

36. The method of claim 28, wherein a node comprises one or more wireless devices that are classified as vulnerable.

37. A mobile application security system, comprising:

a mobile application capable of jumping between hosts during execution; and

a management and security node, in communication with the hosts, the management and security node configured to determine whether to authenticate a user of a dispatching host prior to dispatch of the mobile application responsive to a vulnerability classification of the dispatching host and a sensitivity classification of the mobile application, and request authentication if authentication of the user is required.

38. The mobile application security system of claim 37 wherein the management and security node requests the authentication responsive to the dispatching host being classified as vulnerable and the mobile application being classified as sensitive.

39. The mobile application system of claim 38 wherein the dispatching host is classified as vulnerable if comprising one from the group containing a wireless device, a mobile device, a handheld device, and a laptop computer.

40. The mobile application security system of claim 37 wherein the management and security node does not request the authentication of the mobile application responsive to the dispatching host being classified as non-vulnerable or the mobile application being classified as non-sensitive.

41. The mobile application system of claim 37 wherein the management and security node receives the mobile application from the dispatching host, and dispatches the mobile application to the receiving host responsive to determining that the authentication is not required or authenticating the mobile application.

42. The mobile application security system of claim 37 wherein the management and security node authenticates the mobile application including receiving a first authentication data prior a jump, receiving a second authentication data during the jump, and comparing the first and second authentication data.

43. The mobile application security system of claim 37 wherein the management and security node authenticates the dispatching host.

44. The mobile application security system of claim 37herein the management and security node authenticates the dispatching host prior to dispatch.

45 The mobile application security system of claim 37 wherein the hosts do not include the management and security node.

46 The mobile application security system of claim 37 further comprising a host.

47 A mobile application security system, comprising:

a mobile application capable of jumping between hosts during execution; and

a dispatching host, in communication with a management and security node, the dispatching host configured to provide a vulnerability classification of the dispatching host and a sensitivity classification of the mobile application to the management and security node prior to dispatch in order to determine whether authentication of a user of the dispatching host is required, and to assist authentication of the user responsive to receiving an authentication request.

48 The mobile application security system of claim 47 wherein the dispatching host sends authentication information to the management and security node to perform the authentication.

49 The mobile application security system of claim 47 wherein the dispatching host dispatches the mobile application to the management and security node.

--

Any inquiry concerning this communication of earlier communication form the examiner should be directed to Peter Poltorak whose telephone number is (871) 272-3840. The examiner can normally be reached reached Monday through Thursday from 8:00 a.m. to 5:30 p.m. and alternate Fridays from 8:00 a.m. to 4:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis Jacques can be reached on (571) 272-6962. The fax

phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

7/7/06

JACQUES LOUIS-JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100